Document number: D0000000771
Name: Product Security Risk Analysis Techniques
Revision: AB

Work instruction

Table of contents

Work instruction

1. Purpose

1.1. This work instruction provides guidance and instructions for applying product security risk analysis as part of risk management per CQP-RSK-001.

2. Scope

2.1. This work instruction applies to medical devices for which Stryker owns the product design and which include software as defined in CQP-DLC-008.

2.2. This work instruction applies to the following functions:

2.2.1. Product Development

2.2.2. Post Market Surveillance.

3. References

3.1. Internal references

3.1.1. CQP-RSK-001, *Risk management*

3.1.2. CQP-DLC-008, *Software life cycle process*

3.1.3. D0000000909, *Product security risk table*

3.1.4. D0000003422, *Product security standard assessment*

3.2. External references

3.2.1. AAMI TIR57:2016, *Principles for Medical Device Security – Risk Management*

3.2.2. NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*

3.2.3. FDA Guidance for Industry and Food and Drug Administration Staff October 2, 2014, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*

3.2.4. FDA Guidance for Industry and Food and Drug Administration Staff December 28, 2016, *Postmarket Management of Cybersecurity in Medical Devices*

3.2.5. ISO 14971, *Medical Devices – Application of Risk Management to Medical Devices*

3.2.6. EN ISO 14971, *Medical Devices – Application of Risk Management to Medical Devices*

3.2.7. ISO 27799:2016, *Health informatics -- Information security management in health using ISO/IEC 27002*

Work instruction

4. Definitions

4.1. Refer to CQM-02, *Stryker Corporation Quality and Regulatory Master Glossary*.

4.1.1. Component

4.1.2. Establish

4.1.3. Harm

4.1.4. Medical device

4.1.5. Process(es)

4.1.6. Risk

4.1.7. Risk Analysis

4.1.8. Risk Assessment

4.1.9. Risk Evaluation

4.1.10. Risk Control

4.1.11. Risk Management

4.1.12. Risk Management File

4.1.13. Risk Matrix

4.1.14. Risk Table

4.1.15. Verification

4.2. Locally defined terms

4.2.1. Adversarial threat source - Type of threat source with adversarial intent.

4.2.2. Adverse impact - The impact that the loss of confidentiality, integrity, or availability might have on safety, effectiveness, or data and system security.

4.2.3. Asset - Person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

4.2.4. Attack complexity - Metric that describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability and require collection of more information about the target. The metric is a required component to calculate the CVSS 3.0 score.

4.2.5. Attack tree - Technique that can be used in security risk assessments to assess the risk of a security violation from one of many possible attacks or from a combination of attacks.

4.2.6. Attack Vector - The method that malicious code such as viruses or worms uses to propagate itself or infect a software system.

4.2.7. Availability - Timely and reliable access to and use of information.

4.2.8. Capability - The ability or means necessary for a threat actor to exploit the vulnerability.

4.2.9. Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

4.2.10. CVSS 3.0 - Open industry standard for assessing the severity of computer system security vulnerabilities, maintained by the Forum of Incident Response and Security Teams (FIRST). The US National Vulnerability Database uses CVSS scoring to rank critical vulnerabilities

4.2.11. CVSS 3.0 base score - The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity. The CVSS v3.0 base score is used as the baseline scheme to produce a numerical score to do security risk estimation and evaluation. The CVSS v3.0 base score is composed of two sets of metrics, the exploitability metrics and the technical impact metrics.

4.2.12. Exploitability - The capability necessary for a threat actor to exploit the vulnerability.

4.2.13. Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

4.2.14. Intent - The motivation of a threat source to initiate a threat event.

4.2.15. Impact to safety - Impact causing harm.

4.2.16. Non-adversarial threat source - Type of threat source with non-adversarial intent.

4.2.17. Privileges - Access rights granted to a user, program, or process.

4.2.18. Targeting - Adversaries actively selecting a specific device or component for exploitation of a vulnerability

4.2.19. Technical Impact - The impact on confidentiality, integrity, or availability of a technical system.

4.2.20. Threat - Threat is any circumstance or event with the potential to adversely impact the device, organizational operations ..., organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or essential performance of the device.

4.2.21. Threat actor - Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

4.2.22. Threat event - Event or situation that has the potential for causing undesirable consequences or impact.

4.2.23. Threat event initiation - The initiation of a threat event.

4.2.24. Threat source - Intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

4.2.25. Vulnerability - Weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat.

5. Roles and responsibilities

5.1. Design Engineering (R&D)

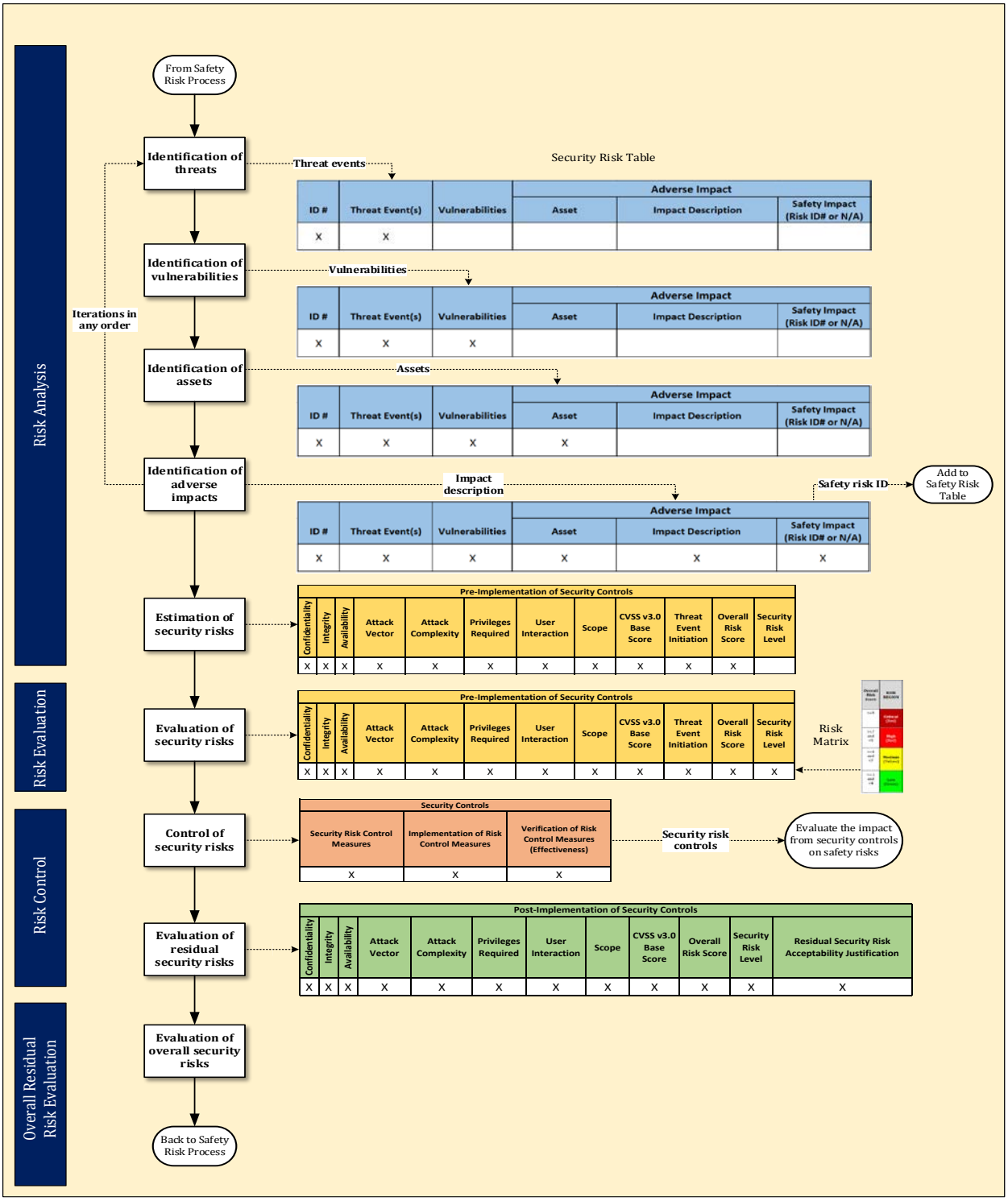
5.1.1. Responsible for conducting the security risk analysis activities and providing subject matter expertise on product design and security.

5.2. Quality Assurance

5.2.1. Responsible for all product safety risk management activities. Supporting the product security risk team on all aspects related to safety.

Work instruction

6. Process flow



Work instruction

7. Work instruction

7.1. General requirements

7.1.1. If product security is in the scope of the product under consideration a product security risk analysis **shall** be performed in accordance with this instruction under the umbrella of CQP-RSK-001.

Note: Figure 1 shows the relation between security and safety risk.

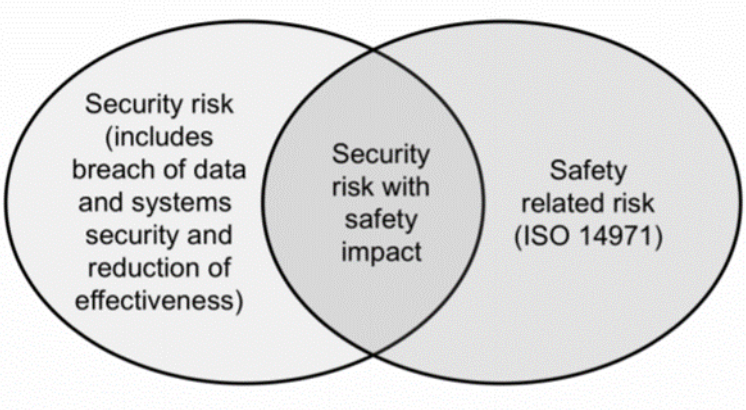


Figure 1: Safety risk and security risk relation

7.1.2. The following activities are required elements of the security risk management process and **shall** be conducted and documented per section 7 of this work instruction and in accordance with CQP RSK-001:

7.1.2.1. Identification of threats

7.1.2.2. Identification of vulnerabilities

7.1.2.3. Identification of assets

7.1.2.4. Identification of adverse impacts

7.1.2.5. Estimation of security risks

7.1.2.6. Evaluation of security risks

7.1.2.7. Control of security risks

7.1.2.8. Evaluation of residual security risks

7.1.2.9. Evaluation of overall residual security risk acceptability.

7.1.3. Product security risk analysis results, including the description and identification of the medical device, **shall** be documented using the security risk table D0000000909.

7.1.4. The identification of threats, vulnerabilities, assets, and adverse impacts **may** be performed in any order.

7.1.5. Libraries which catalog known assets, possible threats and possible/known vulnerabilities **may** be cataloged for future consideration per divisional practice.

7.1.6. The following types of supporting documents **should** be reviewed during the identification activities as they may all serve as an input to asset, vulnerability or threat identification.

7.1.6.1. Functional analysis

7.1.6.2. DIOV trace matrix

7.1.6.3. Risk Table

7.1.6.4. Medical device/scope diagram

7.1.6.5. FMEA/FMECA

7.1.6.6. Software Architectural Design (SAD)

7.1.6.7. Software Requirements Specifications (SRS)

7.1.6.8. Software Bill of Material (SBOM).

7.2. Identification of threats

7.2.1. The threats in scope of the product **shall** be identified and documented.

7.2.2. Threats **may** be identified using the following sources, including but not limited to:

7.2.2.1. Threat Modeling/Mapping, such as OWASP Threat Risk Modeling

Note: A threat model **should** include the identification of potential threat agents, impacts the threat agent is looking to cause, any potential affected assets the threat agent may target to carry out the attack, the motivation of the threat agent, skill level necessary to carry out the attack (e.g., significant training or knowledge with extensive experience), and attack vectors.

7.2.2.2. Standard threat libraries, such as NIST SP 800-30 and ISO 27799

7.2.2.3. Governmental agencies (such as ICS-CERT), Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs)

7.2.2.4. Product/component reviews

A. Review of system components, users and communication pathways where a threat may be introduced.

B. Known vulnerabilities from predicate devices, and vulnerabilities brainstorming

Note 1: Threats **should** be considered an input for the types of vulnerabilities which are considered.

Note 2: Outside sources such as Common Attack Pattern Enumeration and Classification (CAPEC), Common Vulnerabilities and Exposure (CVE), or Common Weakness Enumeration (CWE) **should** be consulted for any new threat sources.

7.2.3. Threat sources **shall** be inclusive of adversarial and non-adversarial threats sources. See Appendix C for examples of threat sources.

7.2.4. Threat identification **shall** include assignment of an ID#, the threat event, a description explaining the threat event, the threat source, and the assessment for applicability. A rationale **shall** be provided for any threats considered out of scope for the device. See Appendix C for threat event examples.

7.3. Identification of vulnerabilities

7.3.1. Known and potential vulnerabilities in scope of the product **shall** be identified and documented.

7.3.2. Vulnerabilities **may** come from three distinct sources

7.3.2.1. Introduced by conscious design decisions

7.3.2.2. Errors in design, implementation, manufacture, or configuration of the device

7.3.2.3. Design characteristics that at the time of design release was not known to be a vulnerability, but subsequent to design release a means of exploiting the design characteristics for malicious purposes was discovered (i.e. post market release).

7.3.3. Vulnerabilities **may** be identified by incorporating top-down analysis methodologies (e.g. attack trees, threat modeling, and fault tree analysis) to identify ways that a threat can cause loss of security properties for the device.

7.3.4. When brainstorming a list of vulnerabilities, the following **should** be considered:

7.3.4.1. Review of system components, users and communication pathways where a vulnerability may be introduced.

7.3.4.2. The Software Bill of Material (SBOM) **should** be reviewed for identification of related vulnerabilities for each component of the software. Recognized vulnerabilities from independent sources (i.e. National Vulnerability Database (NVD) **should** be consulted (cross-checked) when identifying (brainstorming) a list of possible vulnerabilities for the medical device/system.

7.3.4.3. Applicable security capabilities, per D0000003422

7.3.4.4. Knowledge from predicate devices, news sources and previous security testing.

7.3.5. The vulnerability identification **shall** include assignment of an ID#, a description of the vulnerability, and the assessment for applicability. A rationale **shall** be provided for any vulnerabilities considered out of scope for the device. See Appendix B for vulnerability examples.

7.4. Identification of assets

7.4.1. The assets in scope of the product **shall** be identified and documented.

7.4.2. Assets **shall** include as applicable to the medical device:

7.4.2.1. Information (i.e. patient data, diagnostic data)

7.4.2.2. The device itself, or components of the device (including device software)

7.4.2.3. Physical interfaces of the device (i.e. connections to external networks).

7.4.3. Assets **should** include those assets needed by the user to manage, diagnose and treat the patient, as well as those assets required to keep the device operating safely and securely.

7.4.4. Particular attention **shall** be on stored authentication or cryptographic credentials that are used by the device.

7.4.5. Assets **should** include those to be the target of value for a threat source. This includes those assets that would be attractive for an attacker providing the ability to accomplish their goals based on their motivations.

7.4.6. Asset identification **shall** include assignment of an ID#, asset type and a description of the asset. See Appendix A for asset examples.

7.5. Identification of adverse impacts

7.5.1. For each identified asset, the impact that the loss of confidentiality, integrity, or availability might have on safety, effectiveness, or data and system security, **shall** be documented.

7.5.2. The relevance of the impact to safety **shall** be evaluated. If the impact could result in an S1 or higher harm, traceability to the corresponding risk id in the Risk Management File **shall** be established.

Note: For a definition of the severity levels of harm refer to the risk matrix in CQP-RSK-001.

7.6. Estimation of security risks

7.6.1. For each applicable combination of the threat event, vulnerability, and impact of asset compromise:

7.6.1.1. The technical impact to confidentiality, integrity, and availability **shall** be assessed in accordance with Appendix E.

7.6.1.2. The exploitability **shall** be assessed in accordance with Appendix D.

7.6.1.3. A CVSS v3.0 base score **shall** be calculated in accordance with Appendix F.

7.6.1.4. A threat event initiation factor considering the characteristics of the threat source and the associated threat initiation score **shall** be assessed in accordance with Appendix C.

7.6.1.5. An overall risk score **shall** be calculated as a combination of the CVSS v3.0 base score and the threat event initiation score in accordance with Appendix G.

Note: The CVSS v3.0 base score may differ from a customer provided CVSS score, or NVD CVSS score, due to the CVSS v3.0 score considering Stryker specific assets.

7.7. Evaluation of security risks

7.7.1. For each security risk line item, the corresponding risk region based on the overall risk score **shall** be documented in the security risk table and **shall** be evaluated according to Table 1 to decide if risk reduction is necessary.

Work instruction

Table 1: Product Security Risk Matrix

Overall Risk Score (Range 0 to 10)	RISK REGION	***Part I:*** ***Pre-Implementation of Security Controls***	***Part II:*** ***Post-Implementation of Security Controls***	
			Impact on safety	***No impact on safety (business risk only)***
<= 10 and >=9	**Critical** (Red)	Risk reduction is necessary. Risk control option analysis is required.	Evaluation per CQP-RSK-001	Residual business risk is unacceptable unless business risk has been reduced as much as reasonably practicable and business risk/benefit analysis indicates that the residual business risk is judged acceptable.
<9 and >=7	**High** (Red)			
<7 and >=4	**Medium** (Yellow)			
<4 and >=0.1	**Low** (Green)	Risk reduction is not necessary, unless known to be possible*.	=	Risk is broadly acceptable.
= 0	**None** (Gray)			

* According to the generally acknowledged technological state of the art for similar medical devices.

7.8. Control of security risks

7.8.1. Security risk control options **shall** be analyzed using the following hierarchy:

7.8.1.1. Inherent security by design

7.8.1.2. Protective measures in the medical device itself or in the manufacturing process

7.8.1.3. Information for security.

Note: A security risk control measure **may** mitigate a threat, vulnerability or impact.

7.8.2. The selected security risk controls **shall** be implemented and documented in the security risk table.

7.8.3. Implementation of each risk control **shall** be verified and documented in the security risk table.

7.8.4. Effectiveness of each risk control **shall** be verified and documented in the security risk table.

7.9. Evaluation of residual security risks

7.9.1. For each security risk the overall risk score **shall** be re-assessed per section 7.6 after the risk controls have been applied.

7.9.2. For each security risk the residual security risk level **shall** be evaluated per Table 1 to decide if residual risks are acceptable or if further risk reduction is necessary after the security risk controls have been applied.

7.9.3. Security risks that impact safety **shall** be evaluated against the acceptability criteria per CQP-RSK-001.

7.9.4. Security risks that do not impact safety **shall** be evaluated based on a business risk/ benefit analysis per divisional practice.

7.9.5. After risk reduction activities, security risk controls **shall** be evaluated for the following:

7.9.5.1. Impact on safety (i.e. increase in occurrence level, severity level or introduction of a new risk)

7.9.5.2. Possible introduction of new security risks.

7.9.6. Risk control measures, per CQP-RSK-001, applied to the medical system for safety **shall** be reviewed for impact to security risk management.

7.9.7. After all security risk controls are implemented and verified, completeness of risk control **shall** be confirmed by ensuring that the risks from all identified threats, vulnerabilities, and potentially compromised assets have been considered and documented in the security risk table.

7.10. Evaluation of overall residual security risk acceptability

7.10.1. The overall residual security risk **shall** be evaluated per CQP-RSK-001.

Work instruction

8. Appendices

8.1. Appendix A, *Asset examples*

8.2. Appendix B, *List of example vulnerability categories and vulnerability types*

8.3. Appendix C, *List of example threat sources, threat event guidance, and threat event initiation*

8.4. Appendix D, *CVSS v3.0 Exploitability metrics*

8.5. Appendix E, *CVSS v3.0 Scope and technical impact metrics*

8.6. Appendix F, *CVSS v3.0 base score*

8.7. Appendix G, *Overall risk score*

Appendix A

Asset examples[1]

Physical assets

a) User Interface
b) Device assets
    1) Operating system
    2) Software libraries
    3) Application software
    4) Keys/Certificates
    5) Device identity
    6) Device resources
        i. Processing
        ii. Memory
        iii. I/O
    7) Physical interfaces
c) Device telemetry
d) Network interface

Information assets

a) Patient data
b) HDO data
c) Insurance/coverage data
d) Device settings/ programming commands
e) Passwords
f) Configurations
    1) Network
    2) Infrastructure
g) Diagnostic logs
h) Physical location
i) Telemetry data
j) Session credentials (keys, tokens, etc.)

[1] Source: AAMI TIR 57:2016, Annex B

Appendix B

List of example vulnerability categories and vulnerability types[2]

Vulnerability category	Vulnerability Type	Example Vulnerability
Physical Environment	Information display	Patient information displayed on screen
	Physical Security	Inability to detect a physically connected simulator
	Power availability	Inability to turn on/off device
Personnel	Users	Utilization of feature not controlled by privileges (e.g. sending messages)
	Developers	Application has admin privileges upon boot up
	Support Staff	Support staff have admin privileges
Hospital/Facility	Security Measures	Customer organizational security practices not implemented or utilized
	Administrative Procedures	Customer organizational security procedures do not adequately restrict physical or remote access
Business Operation and service delivery	Business Operation and service delivery	Unauthorized personnel have access to service/maintenance keys
Hardware	Debug interfaces enabled	System susceptible to overload
	Use of removable media	Connected external media can be compromised or introduce malware into system
	Lack of physical tamper detection and response	Physical tampering of device can go undetected
Software	Memory safety violations	Over-write of adjacent memory; loss of data/information
	Input validation error	Malicious data from external entity or client is trusted
	Race conditions	Actions/steps able to be inserted between steps of the secure program
	Privilege-confusion	Unauthorized utilization thought to be under privilege control
	User interface failures	UI does not warn or prevent user initiating unsafe actions to the system
Communication equipment and facilities	Side channels	Memory leak

[2] List partially derived from AAMI TIR57:2016 Annex B

Appendix C

List of example threat sources[3], threat event guidance[4], and threat event initiation[5]

List of example threat sources:

Threat Source Type	Threat Source
Adversarial	Nation States
	Organized Crime
	Disgruntled/ex-employees
	Political activists
	Emotionally unstable
	Script Kiddies
Non-adversarial	Academic researchers
	Professional security researchers
	Unintentional misuse (by users, maintenance or installers)
	Natural events
	Integration effects (i.e. RF interference, incompatible software)

Threat event guidance:

The following are steps that threat actors may take to penetrate a system:

- Reconnaissance - collecting intelligence about the system;
- Penetration - gaining access to the system;
- Enumeration - discovering other system resources; reconnaissance from within the system;
- Execution - conducting a computer network attack or computer network exploitation;
- Maintenance - maintaining access to the system by importing tools and installing backdoors; and
- Concealment - obfuscating to prevent discovery of the exploit or the access tools.

Threat event initiation:

Threat event initiation by taking into consideration the characteristics of the threat sources of concern including capability, intent, and targeting. If threat events require more capability than adversaries possess then the adversaries are not expected to initiate the events. If adversaries do not expect to achieve intended objectives by executing threat events, then the adversaries are not expected to initiate the events. If adversaries are not actively targeting specific device/component, adversaries are not expected to initiate threat events.

[3] Source: AAMI TIR 57:2016, Annex B

[4] Source: AAMI TIR 57:2016, Annex B

[5] List partially derived from NIST SP 800-30:Rev1

Work instruction

Qualitative Values	Threat Event Initiation Score (TEIS)	Treat Event Initiation	Adversarial Threat Sources CAPABILITY, INTENT & TARGET are variable	Non-Adversarial Threat Sources
Very High	1.00	Adversary is **almost certain** to initiate the threat event. (Adversarial) Error, accident, or act of nature is **almost certain** to occur (Non-Adversarial)	Threat source has very sophisticated level of expertise and resources available **AND/OR** Threat source seeks to undermine/impede/destroy a core mission or function of the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure. **OR** Threat source targets specific functionality with high value, mission-critical information within the medical device, accessory (ies) of the medical device, information system (e.g. hospital network), or infrastructure.	The effects of the error, accident, or act of nature are sweeping, involving almost all of the cyber resources of the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure.
High	0.80	Adversary is **highly likely** to initiate the threat event. Error, accident, or act of nature is **highly likely** to occur (Non-Adversarial)	Threat source has sophisticated level of expertise and resources available **AND/OR** Threat source seeks to undermine/impede aspects of a core mission or function within the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure now or in the future. **OR** Threat source targets specific functionality with high value or critical information within the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure.	The effects of the error, accident, or act of nature are wide-ranging involving most of the cyber resources of the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure.
Moderate	0.50	Adversary is **somewhat likely** to initiate the treat event. Error, accident, or act of nature is **somewhat likely** to occur (Non-Adversarial)	Threat source has adequate expertise and resources **AND/OR** Threat source seeks to disrupt the organization by establishing a foothold within the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure. **OR** Threat source targets high value organizations, medical device, accessory(ies) of the medical device, information system (e.g. hospital network) or infrastructure within the organization and/or key positions within the organization.	The effects of the error, accident, or act of nature are wide-ranging involving significant portion of the cyber resources of the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure.
Low	0.20	Adversary is **unlikely** to initiate the threat event. Error, accident, or act of nature is **unlikely** to occur (Non-Adversarial)	Threat source has limited resources and opportunities **AND/OR** Threat source seeks to obtain critical/sensitive information to disrupt the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure. **OR** Threat source seeks targets of opportunity within high value organizations and/or medical device, accessory(ies) of the medical device, information	The effects of the error, accident, or act of nature are limited involving some of the cyber resources of the medical device, accessory(ies) of the medical device, information system

			system (e.g. hospital network) or infrastructure within the organization, through publicly available information	(e.g. hospital network), or infrastructure.
Very Low	0.04	Adversary is **highly unlikely** to initiate the threat event. Error, accident, or act of nature is **highly unlikely** to occur (Non-Adversarial)	Threat source does not have adequate expertise or resources **AND/OR** Threat source seeks to disrupt or deface the organizations, and/or medical device, accessory(ies) of the medical device, information system (e.g. hospital network) or infrastructure within the organization. **OR** Threat source may or may not have specific targets	The effects of the error, accident, or act of nature are minimal involving few if any of the cyber resources of the medical device, accessory(ies) of the medical device, information system (e.g. hospital network), or infrastructure.

Appendix D

CVSS v3.0 Exploitability metrics

Exploitability metrics listed below for the vulnerable component reflects the properties of the vulnerability that lead to a successful attack (Refer to https://www.first.org/cvss/user-guide).

Attack Vector (AV)

This metric reflects the context by which vulnerability exploitation is possible. This metric value (and consequently the base score) will be larger the more remote (logically, and physically) an attacker can be, in order to exploit the vulnerable component.

Metric Value	Description
Network (N)	A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer). Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away (e.g. across layer 3 boundaries from routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet from across the public Internet (e.g. CVE 2004 0230).
Adjacent (A)	A vulnerability exploitable with adjacent network access means the vulnerable component is bound to the network stack, however the attack is limited to the same shared physical (e.g. Bluetooth, IEEE 802.11), or logical (e.g. local IP subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g. a router). An example of an Adjacent attack would be an ARP (IPv4) or neighbor discovery (IPv6) flood leading to a denial of service on the local LAN segment. See also CVE 2013 6014.
Local (L)	A vulnerability exploitable with Local access means that the vulnerable component is not bound to the network stack, and the attacker's path is via read/write/execute capabilities. In some cases, the attacker may be logged in locally in order to exploit the vulnerability, otherwise, she may rely on User Interaction to execute a malicious file.
Physical (P)	A vulnerability exploitable with Physical access requires the attacker to physically touch or manipulate the vulnerable component. Physical interaction may be brief (e.g. evil maid attack [1]) or persistent. An example of such an attack is a cold boot attack which allows an attacker to access to disk encryption keys after gaining physical access to the system, or peripheral attacks such as Firewire/USB Direct Memory Access attacks.

Attack Complexity (AC)

This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability and require collection of more information about the target. This metric value is largest for the least complex attacks.

Metric Value	Description
Low (L)	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.
High (H)	A successful attack depends on conditions beyond the attacker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected. 2 For example, a successful attack may depend on an attacker overcoming any of the following conditions: - The attacker must conduct target-specific reconnaissance. For example, on target configuration settings, sequence numbers, shared secrets, etc. - The attacker must prepare the target environment to improve exploit reliability. For example, repeated exploitation to win a race condition, or overcoming advanced exploit mitigation techniques. - The attacker must inject themselves into the logical network path between the target and the resource requested by the victim in order to read and/or modify network communications (e.g. man in the middle attack).

Privileges Required (PR)

This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability. This metric is greatest if no privileges are required.

Metric Value	Description
None (N)	The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.
Low (L)	The attacker is authorized with (i.e. requires) privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with Low privileges may have the ability to cause an impact only to non-sensitive resources.
High (H)	The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

User Interaction (UI)

This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner. This metric value is greatest when no user interaction is required.

Metric Value	Description
None (N)	The vulnerable system can be exploited without interaction from any user.
Required (R)	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited. For example, a successful exploit may only be possible during the installation of an application by a system administrator.

Appendix E

CVSS v3.0 Scope and technical impact metrics

Scope Change (SC)

Ability for a vulnerability in one software component to impact resources beyond its means, or privileges. This consequence is represented by the metric Scope. When the vulnerability of a software component governed by one authorization scope is able to affect resources governed by another authorization scope, a Scope change has occurred (Refer to https://www.first.org/cvss/user-guide).

Metric Value	Description
Unchanged (U)	An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.
Changed (C)	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the vulnerable component and the impacted component are different.

Confidentiality Impact (CI)

This metric measures the impact to the confidentiality of the information/data resources managed by a software component due to a successfully exploited vulnerability. This metric value increases with the degree of loss to the impacted component.

Metric Value	Description
High (H)	There is total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact. For example, an attacker steals the administrator's password, or private encryption keys of a web server.
Low (L)	There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is constrained. The information disclosure does not cause a direct, serious loss to the impacted component.
None (N)	There is no loss of confidentiality within the impacted component.

Integrity Impact (II)

This metric measures the impact to integrity of information/data by a successfully exploited vulnerability. This metric value increases with the consequence to the impacted component.

Metric Value	Description
High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
None (N)	There is no loss of integrity within the impacted component.

Availability Impact (AI)

This metric measures the impact to the availability of the resources or the component itself resulting from a successfully exploited vulnerability. This metric value increases with the consequence to the impacted component.

Metric Value	Description
High (H)	There is total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained (while the attacker continues to deliver the attack) or persistent (the condition persists even after the attack has completed). Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted component (e.g., the attacker cannot disrupt existing connections, but can prevent new connections; the attacker can repeatedly exploit a vulnerability that, in each instance of a successful attack, leaks a only small amount of memory, but after repeated exploitation causes a service to become completely unavailable).
Low (L)	There is reduced performance or interruptions in resource availability. Even if repeated exploitation of the vulnerability is possible, the attacker does not have the ability to completely deny service to legitimate users. The resources in the impacted component are either partially available all of the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.
None (N)	There is no impact to availability within the impacted component.

Appendix F

CVSS v3.0 base score

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity. The CVSS v3.0 base scoring is used as the baseline scheme to produce a numerical score to do security risk estimation and evaluation (refer to https://www.first.org/cvss/specification-document).

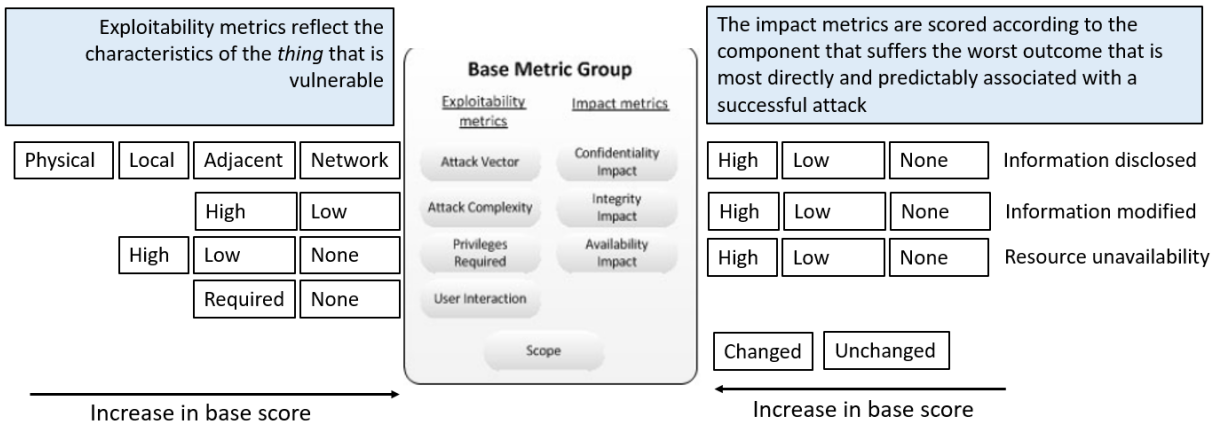
The CVSS v3.0 base score is composed of two sets of metrics, the exploitability metrics and the technical impact metrics including scope change (SC) to reflect an impact to a separate software, hardware, or networking component other than the impacted component.

The exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. The metric assesses the following properties of exploitability, attack vector (AV), attack complexity (AC), privileges required (PR) and user interaction (UI). (Refer Appendix D)

The technical impact metrics reflect the direct consequence of a successful exploit and represent the final worst outcome that is most directly and predictably associated with a successful attack. The confidentiality (CI) impact and integrity impact (II) refer to effect on any data under consideration whereas the availability (AI) impact refers to the performance and operation of the device or component under consideration. (Refer Appendix E)

If a scope change has not occurred, the impact metrics should reflect the confidentiality, integrity, and availability impact to the vulnerable component. However, if a scope change has occurred, then the impact metrics should reflect the CIA impact to either the vulnerable component, or the impacted component, whichever suffers the most severe outcome.

The base metric score ranges from 0.0 to 10.0. The base metric score is derived from exploitability score and impact score including scope change.



Work instruction

For each metric attribute a numerical value is assigned, based on which final CVSS v3.0 base score is calculated. Below is the table listing numerical values for each attribute and equations for CVSS v3.0 base score calculation:

Metric	Metric Value	Numerical Value
Attack Vector / Modified Attack Vector	Network Adjacent Network Local Physical	0.85 0.62 0.55 0.2
Attack Complexity / Modified Attack Complexity	Low High	0.77 0.44
Privilege Required / Modified Privilege Required	None Low High	0.85 0.62 (0.68 if Scope / Modified Scope is Changed) 0.27 (0.50 if Scope / Modified Scope is Changed)
User Interaction / Modified User Interaction	None Required	0.85 0.62
C,I,A Impact / Modified C,I,A Impact	High Low None	0.56 0.22 0

The CVSS v3.0 base score is a function of the impact and exploitability sub score equations. Where the CVSS v3.0 base score is defined as:

CVSS v3.0 base score = (ISCBase <= 0) 0 else,

{Scope Unchanged: Round up (Minimum [(Impact + Exploitability),10])} or

{Scope Changed: Round up (Minimum [1.08 × (Impact + Exploitability),10])}

and the Impact sub score is defined as:

Impact = {Scope Unchanged: 6.42 × ISCBase} OR

{Scope Changed: 7.52 × [ISCBase −0.029] − 3.25 × [ISCBase −0.02]15}

ISCBase = 1 - [(1− IC) × (1− II) × (1− IA)]

and the Exploitability sub score is:

Exploitability = 8.22 × AV × AC × PR × UI

Appendix G

Overall risk score

Calculation of overall risk score

The overall risk score is a combination of the CVSS v3.0 base score and the threat event initiation score (TEIS) and takes additionally into consideration the likelihood of the initiation of a threat event. It ranges from 0 to 10.

Overall security risk score = (ISCBase <= 0) 0 else,

{Scope Unchanged: Round up (Minimum [(Impact + Exploitability *** TEIS**),10])} or

{Scope Changed: Round up (Minimum [1.08 × (Impact + Exploitability *** TEIS**),10])}

The Exploitability and Impact scores are calculated as defined in Appendix F. The determination of the threat event initiation score (TEIS) is defined in Appendix C.

Signatures for document: Product Security Risk Analysis Techniques

Document Number: D0000000771
Date: 2018-12-18 14:29:17.0
Revision: AB
ECR Number: ECR-08056
ECN Number: ECN-02455

This document has been signed using an electronic signature within Windchill. To access the original source document and relevant information, please access the system directly.

Approval Information				
Group	Approval Role	Name	Date	Vote
	Document Control	Harn Ellen	2018-12-20 15:22:47.0	Approve
	Quality Leadership	Pross Juergen	2018-12-18 14:32:31.0	Approve
	Process Owner	O'Keefe, Tom	2018-12-18 15:20:31.0	Approve